IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | | |
|---|---|---|---|
| Applicant: | Messaoud Benantar | | |
| Assignee: | International Business Machines Corporation | | |
| Title: | Method and System for Network Single Sign-on Using a Public Key Certificate and an Associated Attribute Certificate | | |
| Serial No.: | 09/821,064 | Filing Date: | March 29, 2001 |
| Examiner: | Christopher J. Brown | Group Art Unit: | 2134 |
| Docket No.: | AUS920010140US1 | Customer No. | 65362 |

Austin, Texas
October 2, 2007

FILED ELECTRONICALLY

**PRE-APPEAL BRIEF REQUEST FOR REVIEW AND STATEMENT OF REASONS**

Sir:

Applicant requests review of the Final Rejection dated July 2, 2007 in the above-identified application. No amendments are being filed with the request. The following sets forth a succinct, concise, and focused set of arguments for which the review is being requested.

**CLAIM STATUS**

In the final Office Action, the Examiner rejected claims 1-26 under 35 U.S.C. § 103(a) as being unpatentable over various combinations of U.S. Patent No. 6,691,232 to Wood ("Wood"), U.S. Patent No. 5,339,403 to Parker ("Parker"), U.S. Patent No. 6,766,454 to Riggins ("Riggins"), U.S. Patent No. 5,339,403 to Olden ("Olden"), and U.S. Patent No. 6,754,829 to Butt ("Butt"). On September 4, 2007, Applicant filed an Amendment after Final proposing to amend claims 3, 13 and 21, but these amendments were not entered. *See*, Advisory Action, (September 13, 2007). For the reasons set forth hereinbelow, Applicant respectfully traverses the pending art rejections, and further notes that claim 9 has not been rejected over the cited references, and therefore requests that a notice of allowability be issued for at least claim 9 and claim 10 (which depends from claim 9).

**A. Claims 1, 3, 11, 13, 19 and 21 Are Not Obvious Over Wood and Parker**

In response to the Examiner's rejection of claims 1, 3, 11, 13, 19 and 21 as being obvious over Wood in view of Parker, Applicant respectfully requests reconsideration and withdrawal of

the rejection because the Wood and Parker disclosures do not meet the requirements of claims 1, 3, 11, 13, 19 and 21, and therefore the Examiner has not established a *prima facie* case of obviousness. To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974); In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Where a rejection is based on the assertion that all claim limitations are found in a number of prior art references, the fact finder must determine "[w]hat the prior art teaches, whether it teaches away from the claimed invention, and whether it motivates a combination of teachings from different references." In re Fulton, 391 F.3d 1195, 1199-1200 (Fed. Cir. 2004).

As a preliminary matter, a *prima facie* case of obviousness has not been established because, as noted above, none of the references, alone or in combination, discloses or suggests using a single sign-on (SSO) agent to not only (1) authenticate a user in response to an initial authentication request by obtaining or retrieving an attribute certificate having authentication data for the user, but also to (2) authenticate the user for subsequent authentication requests made by the SSO agent by using authentication data contained within the attribute certificate, as variously recited in claims 1, 11 and 19. *See, e.g.*, claim 1 ("authenticating the user at the SSO agent for the initial authentication request; retrieving by the SSO agent an attribute certificate associated with the user; and authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate.") (emphasis added).

The central role played by the SSO agent is described in the Application as follows:

> [0091] It should be noted that, in the preferred embodiment, the client SSO manager requests and receives an attribute certificate from an attribute certificate authority because it is assumed that the client SSO manager adheres to all PKIX protocols. By obtaining and storing an independently issued attribute certificate, the attribute certificate can be verified as an authenticate certificate by a third-party application. Moreover, if the client SSO manager were to be modified or replaced at some point in time, the attribute certificate could be independently verified as authenticate and then could be used by another SSO application.
>
> * * *
>
> [0093] After obtaining or generating the attribute certificate, thereby completing the configuration phase, user 510 will, at some subsequent point in time, desire to interact with one or more legacy applications 502 on application server 504. Using an appropriate protocol with client SSO manager 510, application server 504 initiates a session for user 500 and requests the user's authentication information for one or more legacy applications. For simplicity of presentation, it can be assumed that the user is initially attempting to access only a single protected resource.

> [0094] Preferably before, but possibly after, initiating the session with the application server, the client SSO manager challenges the user to complete an authentication process. Assuming that the user successfully completes this initial sign-on process, the client SSO manager acts as the user's agent to perform any subsequent authentication processing on behalf of the user.
>
> [0095] Continuing with the example, client SSO manager 510 retrieves attribute certificate 530 containing encrypted authentication attributes 526. Client SSO manager 510 locates the appropriate "SvceAuthInfo" attribute within attribute certificate 530 using the "service" field that corresponds to the legacy application that the user is attempted to access. Client SSO manager 510 then extracts the associated "authinfo" data for the corresponding legacy application.

U.S. Patent Publication No. 2002/0144119 (emphasis added).

The centrality of the SSO agent to the initial and subsequent authentication requests is simply not addressed by either of the cited Wood or Parker references, nor by the Examiner's analysis thereof. In particular, neither reference (or the Examiner's analysis thereof) meets the requirement that the SSO agent use authentication data from the attribute certificate to authenticate the user for subsequent authentication requests, as required in the claims. On this point, Applicant respectfully submits that the rejection analysis in no way acknowledges the specifically-claimed role of the SSO agent in both the initial authentication request and in the subsequent authentications requests. *See*, Final Office Action, p. 3. **Indeed, the cited passage from Wood confirms that, once login credentials are obtained for a user, "the access will typically be allowed without the need for further login credentials and authentication." Wood Patent, col. 6, lines 10-16. Thus, there are no "subsequent authentication requests" in the Wood scheme, much less "authenticating the user for subsequent authentication requests via the SSO agent using authentication data" as claimed. In addition, the cited passage from Parker offered by the Examiner to meet the requirement of an "attribute certificate" (Parker, col. 1, lines 40-50) confirms that the *user*, and not any SSO agent, presents the privilege attribute certificate (PAC) to an application as evidence of the user's access rights.** *See*, Parker, col. 1, lines 40-50 ("According to the invention there is provided a distributed computer system capable of supporting a plurality of users and a plurality of applications, the system including an authentication unit for authenticating a user and issuing that user with a privilege attribute certificate (PAC) which can then be presented to an application **by the user** as evidence of the user's access rights...") (emphasis added). Thus, Parker discloses that the *user* presents the privilege attribute certificate, and suggests no role for an SSO agent in this sequence.

In the Advisory Action comments, the Examiner responds to the dual functional requirements of the SSO agent by asserting that:

> Woods (sic) teaches a single sign on system as shown in Columns 5, and 6 of US 6,691232. Woods teaches an SSO agent made of a login component, gatekeeper component, and other security components. Woods teache (sic, teaches) the user requests authentication from the SSO agent. The SSO agent retrieves from the user a credential such as a certificate, from the request. The SSO agent authenticates the suer (sic, user) for subsequent authentication request by establishing a Trust level, gained from the retrieved certificate.

Advisory Action, (Continuation Sheet). With all due respect, the broad and unspecified citation to two columns of text from the Woods Patent as disclosing "login component, gatekeeper component, and other security components" is entirely too vague and ambiguous for Applicant to understand how Woods allegedly meets the requirement of the claims. For example, the cited passages (including the reference to "login component, gatekeeper component, and other security components," whatever they are) do not meet the specifically-claimed role of the SSO agent in both the initial authentication request and in the subsequent authentications requests. In particular, the selective citation of columns 5 and 6 does not disclose how Woods' "login component, gatekeeper component, and other security components" are used for "authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate" as recited in the claims. Moreover, the Examiner's citation ignores the disclosure in Parker that the *user*, and not any SSO agent, presents the privilege attribute certificate (PAC) to an application as evidence of the user's access rights. *See*, Parker, col. 1, lines 40-50.

As seen from the foregoing (and putting aside for the moment to propriety of combining the Wood and Parker), a *prima facie* case of obviousness has not been established because neither Wood nor Parker disclose or suggest using an SSO agent to both (1) authenticate a user in response to an initial authentication request, and to (2) authenticate the user for subsequent authentication requests using authentication data from an attribute certificate that is retrieved the SSO agent. Accordingly, claims 1, 11 and 19 are allowable. To the extent that dependent claims 3, 13 and 21 each respectively incorporate the requirements of independent claims 1, 11 and 19, these dependent claims are likewise allowable, even though there are additional differences recited in the dependent claims. For at least the foregoing reasons, Applicant respectfully requests that the obviousness rejections of claims 1, 3, 11, 13, 19 and 21 over Wood and Parker be withdrawn and that the claims be allowed.

### B. Claims 2-8, 12-18 and 20-26 Are Not Obvious

In response to the Examiner's rejection of claims 2-8, 12-18 and 20-26 as being obvious over Wood, Parker and Riggins (in the case of claims 2, 5, 12, 15, 20 and 23), Olden (in the case of claims 4, 6, 7, 10, 14, 16, 17, 22, 24 and 25) or Butt (in the case of claims 8, 18 and 26), Applicant respectfully requests reconsideration and withdrawal of the rejections because, as explained above with reference to independent claims 1, 11 and 19, none of the references disclose or suggest using a single sign-on (SSO) agent to not only (1) authenticate a user in response to an initial authentication request by obtaining or retrieving an attribute certificate having authentication data for the user, but also to (2) authenticate the user for subsequent authentication requests made by the SSO agent by using authentication data contained within the attribute certificate, as variously recited in claims 1, 11 and 19. In particular, the deficiencies noted above with respect to Wood and Parker are not remedied by the disclosure of Riggins, Parker or Butt. Putting aside for the moment to propriety of combining these three references, a *prima facie* case of obviousness has not been established because none of the cited references disclose Applicant's use of an SSO agent for authenticating a user for an initial and subsequent authentication requests using authentication data from an attribute certificate obtained by the SSO agent. For at least the foregoing reasons, Applicant respectfully requests that the obviousness rejections of claims 2-8, 12-18 and 20-26 be withdrawn and that the claims be allowed.

## CONCLUSION

In view of the amendments and remarks set forth herein, the application is believed to be in condition for allowance and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the Examiner is requested to telephone the undersigned at (512) 338-9100.

FILED ELECTRONICALLY
October 2, 2007

Respectfully submitted,

*/Michael Rocco Cannatti/*

Michael Rocco Cannatti
Attorney for Applicant
Reg. No. 34,791